Primer parcial 2023 1C
Criptografia - Matematica Aplicada

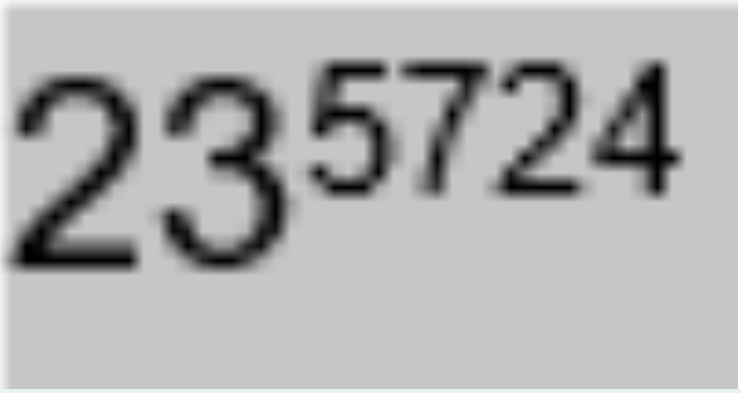
1

¿Cuál de los siguientes puntos es verdadero sobre certificados digitales? *

- (●) Prueba que el suscriptor de un certificado es quien dice ser. CORRECTA
- ( ) Solo se pueden usar los tienen cargados la clave pública de la CA en los navegadores.
- ( ) Es un algoritmo criptográfico que permite generar una clave pública y una privada.
- ( ) No pueden contener datos geográficos.

2

El resto de dividir 23 elevado a 5724 por 3 es: *



- [ ] 0
- [ ] a2
- [x] 1 CORRECTA
- [ ] -1

3

¿Cuál de los cifradores clásicos cumple con el secreto perfecto de Shannon? *

- [ ] Vigenere
- [ ] Playfair
- [ ] Hill
- [x] Vernan CORRECTA

4

Postulados de Golomb - ¿Cuál de los siguientes **no** pertenece a los postulados? *

- [ ] Probabilidad de recibir un 1 o 0 es la misma
- [ ] Sin secuencias con mayor cantidad de información que otras
- [ ] Igual cantidad de unos que de ceros (+/- 1)
- [x] Mayor cantidad de rachas que de huecos CORRECTA

5

5

El algoritmo elegido en el año 2000 como nuevo estándar de cifrado avanzado (AES): *

- Es de tipo Feistel
- Originalmente se llamaba LUCIFER
- Usa Cajas S similares al DES CORRECTA
- Tiene un tamaño de clave fijo de 128 bits

6

La confusión consiste en: *

- Si se cambia un bit en el texto sin cifrar deberían cambiarse la mayor cantidad posible de bits en el texto cifrado
- La relación entre el texto cifrado y la clave sea lo más compleja posible CORRECTA
- Si se cambia un bit en el texto sin cifrar debería cambiar la menor cantidad posible de bits del texto cifrado
- Ninguna opcion es correcta

7

El algoritmo ElGamal *

- [ ] Basa su seguridad en la dificultad de resolución del Problema de la Factorización de Números Grandes (PFNG)
- [ ] Es un algoritmo simétrico
- [ ] Basa su seguridad en la dificultad de resolución del Problema del Logaritmo Discreto (PLD) CORRECTA
- [x] Elimina la necesidad de tener un centro para distribuir llaves

8

Seguridad en Wireless - la siguente afirmacion "Con RADIUS toda la infraestructura Wireless está dentro del firewall corporativo" es: *

- [x] Verdadero CORRECTA
- [ ] Falso

9

¿Cuáles de los siguientes **no** se puede asegurar con criptografía? *

- [ ] Garantía de que un usuario es quien dice ser
- [ ] Comunicaciones seguras
- [ ] Almacenamiento seguro
- [x] Garantía de que un mensaje llegue CORRECTA

10

¿Cuál de las siguientes características es provista por los sistemas simétricos? *

- [ ] No repudio
- [x] Confidencialidad CORRECTA
- [ ] Propagación
- [ ] Disponibilidad

11

El algoritmo de Diffie-Hellman es usado para: *

- [ ] Firma Digital
- [ ] No repudio
- [x] Intercambio de llaves CORRECTA
- [ ] Encripción de archivos

12

¿Cuál sería una **desventaja** de los cifradores en bloque? *

- [ ] Hay una alta difusión en el criptograma
- [x] Se debe leer todo el bloque CORRECTA
- [ ] Baja difusión en el criptograma
- [ ] Imposibilidad de introducir bloques sin detectarlos

13

Protocolos de seguridad en redes - ¿Cuál de las siguentes etapas **no** está al inicio de la comunicación en SSL – Secure Socket Layer? *

- Negociación de clave simétrica de sesión
- Negociación de algoritmos a utilizar
- Intercambio de certificados y autenticación
- Comprobacion de usuario active directory CORRECTA

14

El inverso multiplicativo de 4 en Z_{23} es: *

- No tiene inverso multiplicativo
- 6 CORRECTA
- 8
- 20

15

Protocolos de seguridad en redes - En Kerberos, ¿cuál de las siguientes opciones **no** es un objeto de seguridad? *

- [ ] Tickets
- [ ] Clave de sesion
- [x] MIME CORRECTA
- [ ] Autenticadores

16

¿Cómo se llama al valor de longitud fija usado como huella digital en un mensaje? *

- [ ] MAC
- [x] Hash CORRECTA
- [ ] Mensaje cifrado
- [ ] Firma Digital

17

¿Cuál de las siguientes corresponde a una ventaja del cifrado en flujo? *

- [ ] Ninguna es correcta
- [x] Alta velocidad de cifrado CORRECTA
- [ ] Alta difusión en el criptograma
- [ ] Imposible introducir bits sin detectarlos

18

El cálculo de inverso multiplicativo *

- [x] Es utilizado para aplicar el descifrado de información
- [ ] Es utilizado para aplicar el cifrado de información
- [ ] Ninguna es correcta
- [ ] Es utilizado para realizar el intercambio de claves CORRECTA

19

¿Cuál es el objetivo del proyecto eSTREAM? *

- [ ] Demostrar las debilidades de LFSR
- [ ] Demostrar las debilidades de DES
- [ ] Definir un algoritmo standard para el cifrado en bloque
- [x] Definir un algoritmo standard para el cifrado en flujo CORRECTA

20

¿Qué tipo de cifrador es el cifrador de Cesar? *

- [ ] Trasposición
- [ ] Polialfabético
- [ ] Esteganografía
- [x] Sustitución CORRECTA

21

¿Cuál de las siguientes variantes es más segura en la encripción Triple DES? *

- DES-EDE1
- DES-EDE3 CORRECTA
- DES-EDE2
- DES-EEE4

22

Protocolos de seguridad en redes - ¿Cuál de las siguientes opciones **no** es una cualidad de IPSEC? *

- Permite soportar distintas aplicaciones.
- Es nativa en IP V4 CORRECTA
- Permite armar VPN (Virtual Private Network)
- Puede cifrar y/o autenticar todo el tráfico a nivel IP
- Es transparente para aplicaciones y usuarios

23

Seguridad en Wireless ¿Qué puede hacer un atacante Wireless? *

- [ ] Conseguir Accesos no autorizados
- [x] Todas las opciones son correctas CORRECTA
- [ ] Robo de información
- [ ] Monitoreo, captura y análisis pasivo de tráfico de red
- [ ] Actuar como Man in the Middle

24

¿En qué consiste un ataque analítico? *

- [ ] Se prueban todas las claves posibles
- [x] En la manipulación algebraica para reducir la complejidad
- [ ] En utilizar las debilidades estadísticas del diseño CORRECTA
- [ ] No atacan el algoritmo, sino como fue implantado

25

Los números 624 y 180:
*

- [ ] Son coprimos
- [x] Tienen a 4 como máximo común divisor
- [ ] Son primos
- [ ] Tienen a 12 como máximo común divisor CORRECTA

26

Protocolos de seguridad en redes - En SET – Secure Electronic Transaction las entidades deben instalar instalar el software. ¿Cuál opcion **no** es válida? *

- ( ) Los bancos que procesaban las operaciones
- (•) Las entidades emisoras de las tarjetas de crédito
- ( ) Los comercios adheridos
- ( ) Empresas externas de seguridad controladoras CORRECTA

27

¿Cuál de los siguientes criptosistemas clásicos pertenece al tipo Transposición? *

- (•) Escitala CORRECTA
- ( ) César
- ( ) Vernam
- ( ) Vigenere

28

¿Qué concepto matemático usa como base para la encripción el algoritmo RSA? *

- Curvas elípticas
- Problema del logaritmo discreto
- Matemática discreta
- Grandes números primos CORRECTA

29

Sellado de tiempo – Time Stamping: Se aplica, entre otras cosas, para: *

- Protección de la propiedad intelectual CORRECTA
- Ninguna es correcta
- Establecer comunicación que dura un tiempo determinado
- Intercambio de clave

30

Seguridad en Wireless- ¿Cuál no es un tipo común de EAP? *

- EAP-MD5
- EAP-Cisco Wireless (LEAP)
- EAP-SSH CORRECTA
- EAP-TLS
- EAP-TTLS